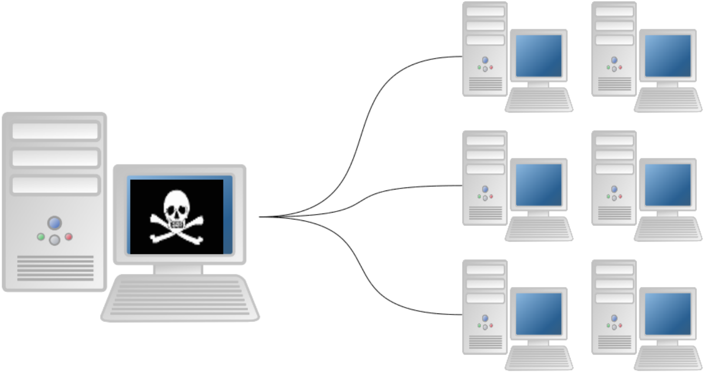
FORTINET

An OpenBTS GSM Replication Jail for Mobile Malware

Axelle Apvrille

Virus Bulletin Conference, October 2011

Malware Jail

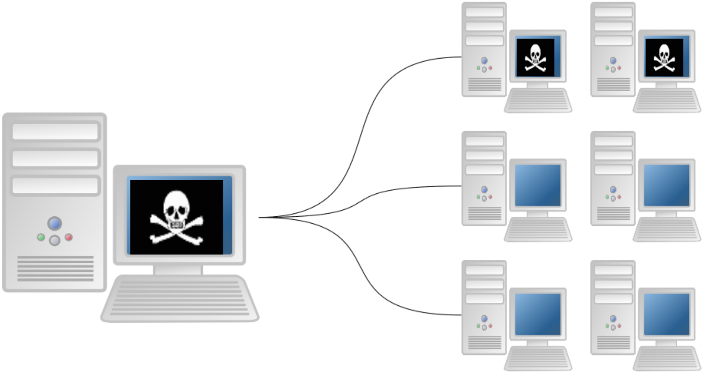


Thou Shalt Not Spread (Nor Leak)

Malware Jail

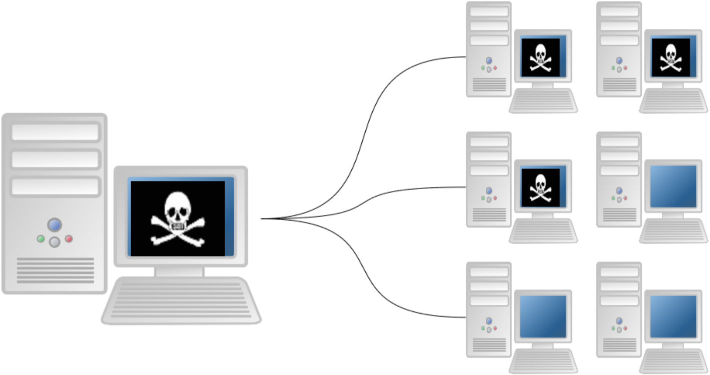
Thou Shalt Not Spread (Nor Leak)

Malware Jail



Thou Shalt Not Spread (Nor Leak)

Malware Jail

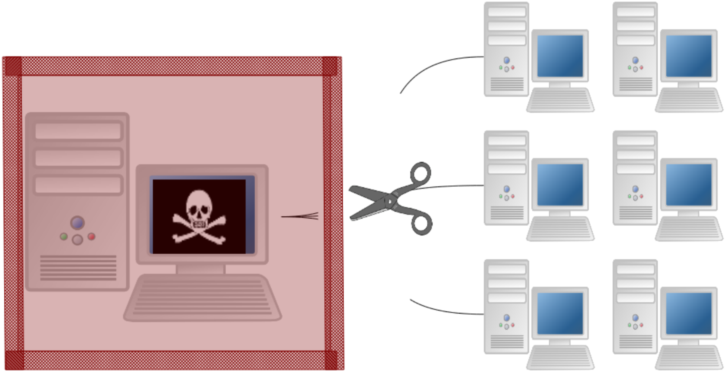


Thou Shalt Not Spread (Nor Leak)

Malware Jail

Thou Shalt Not Spread (Nor Leak)

Malware Jail



Thou Shalt Not Spread (Nor Leak)

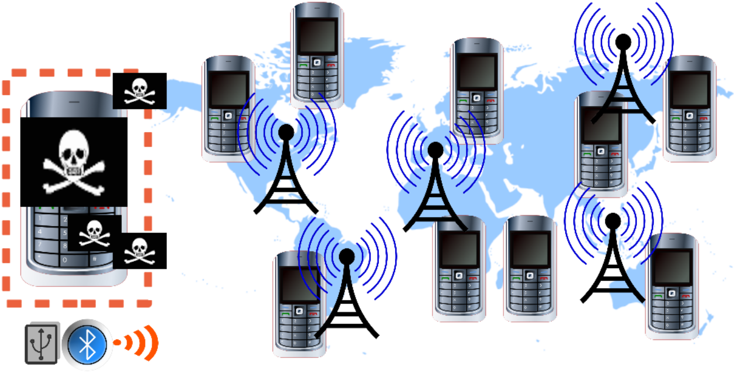
Malware Jail

Thou Shalt Not Spread (Nor Leak)

Malware Jail

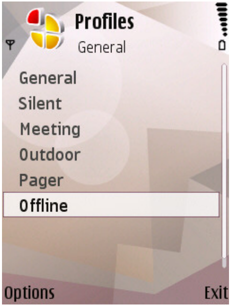
Thou Shalt Not Spread (Nor Leak)

Malware Jail



Thou Shalt Not Spread (Nor Leak)

Jail 1. Remove SIM/ Offline/ Flight mode

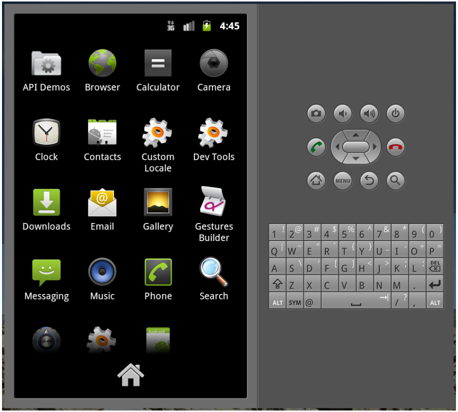


- Secure... probably
- Behaviour: changed!

Malware Name	Online	Offline
SymbOS/Album	Sends 2 SMS	-
SymbOS/Acallno	Trojan spyware	Can't be activated
SymbOS/Feixiang	Sends 2 SMS	Sends 1 SMS
Java/Konov, SymbOS/-ZoomSms	Sends SMS	System lag

Jail 2. Use an emulator

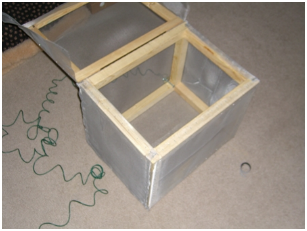
- Good Android emulator, but other OS?
- Same behaviour change problem
- Hardware exploits/ VM detection



Jail 3. Faraday cage

Not that easy to build...

Jail 3. Faraday cage

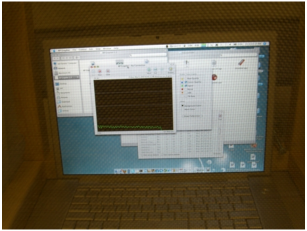


Courtesy of J. Daniels
http://www.jeddaniels.com/2007/faraday-cage-part-1/

Not that easy to build...

- How to see the screen?

Jail 3. Faraday cage

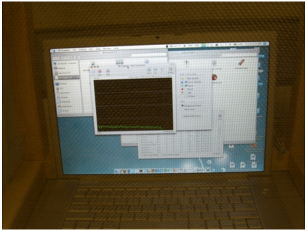


Courtesy of J. Daniels
http://www.jeddaniels.com/2007/faraday-cage-part-1/

Not that easy to build...

- How to see the screen?
- Access to keyboard?

Jail 3. Faraday cage



Courtesy of J. Daniels
http://www.jeddaniels.com/2007/faraday-cage-part-1/

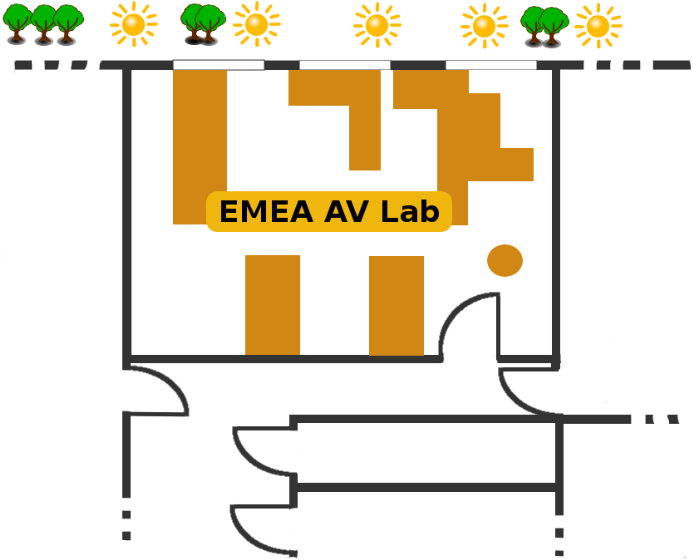
Not that easy to build...

- How to see the screen?
- Access to keyboard?

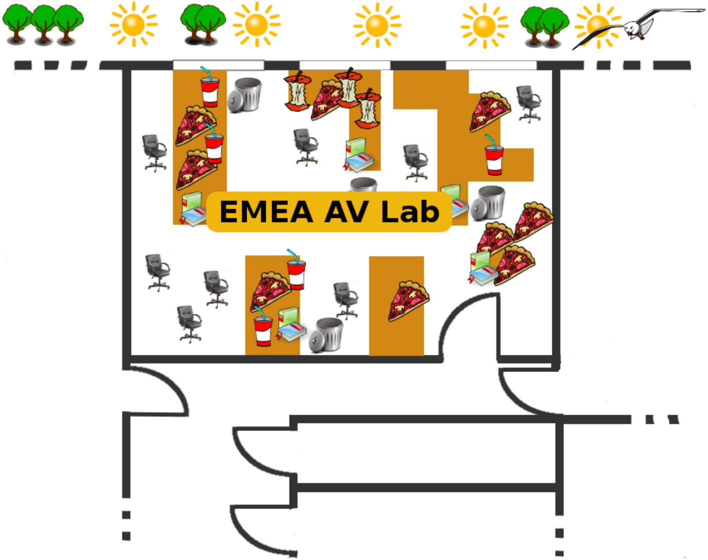
Large Faraday cages

Expensive + Weight

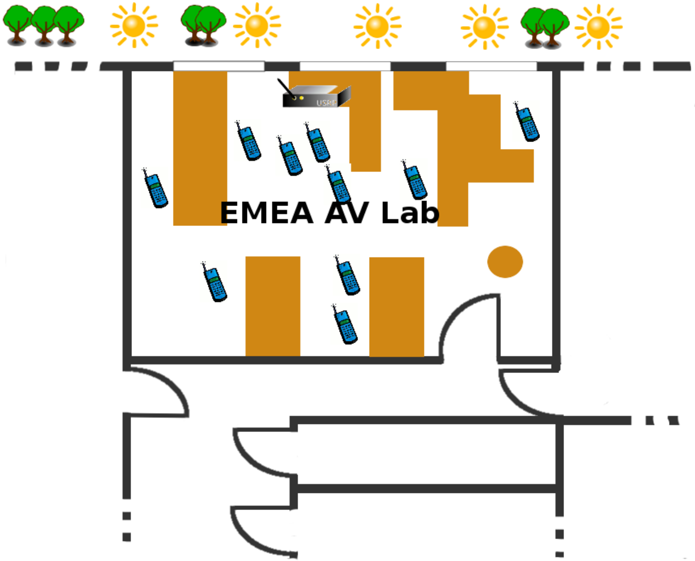
Build your own operator network!



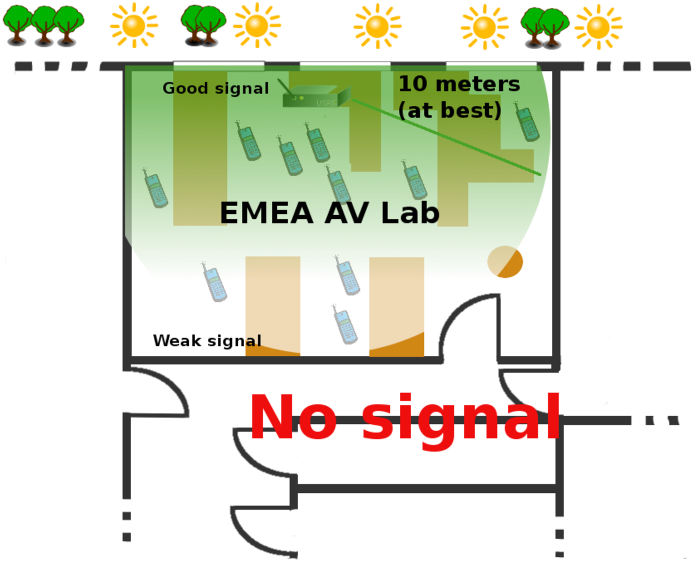
Build your own operator network!



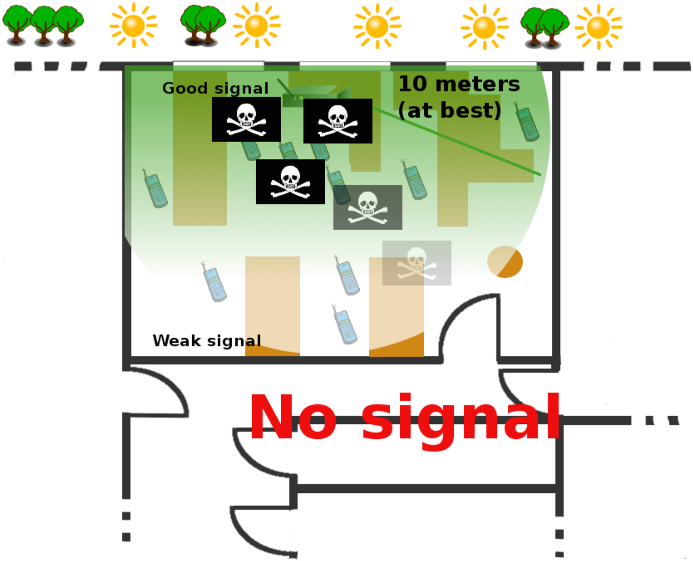
Build your own operator network!



Build your own operator network!



Build your own operator network!



What's OpenBTS?

OpenBTS

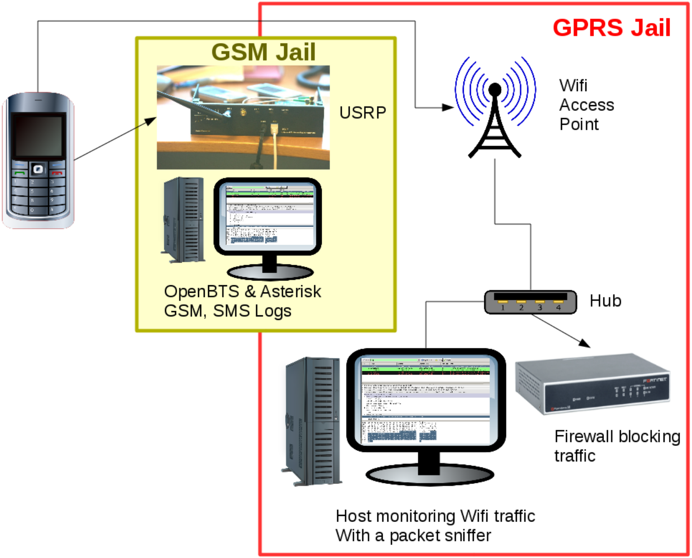
- Open source project
- Local GSM operator = USRP + accurate clock + host running OpenBTS / Asterix
- No GPRS, EDGE, UMTS...

OpenBTS is a registered trademark of Range Networks, Inc.

And nanoBTS-OpenBSC?

Good (perhaps better?)... but 6 times more expensive

Jail Architecture



Video: Using an OpenBTS Jail for Malware Analysis

2103

Infected by Zitmo

2102

Attacker Intercepts SMS

2111

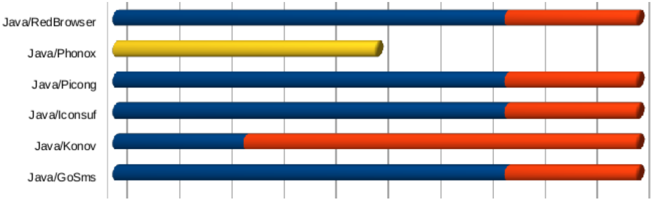
Genuine Friend / Bank Sends SMS to infected

What the analyst sees...

Part 1. ... when the phone is offline

Part 2. ... with an OpenBTS-based jail

Results



Blue: offline, Red: with GSM jail, Yellow: +GPRS jail.

Full results: see paper.

Main Advantages

- Behaviour similar to real conditions
- See SMS contents and details
- No leak to real networks
- Low cost

Limitations

- Sample requires a WCDMA bearer
- MMS not handled
- Dynamic analysis limitations

Thank You !

Follow us on http://blog.fortinet.com
or twitter: **@FortiGuardLabs**

Axelle Apvrille

aka *Crypto Girl*
/mobile malware reverse engineering/
aapvrille@fortinet.com

Slides edited with LOBSTER